12 novedades del nuevo reglamento de protección de datos que las empresas deberían tener en cuenta

Empresas y autónomos españoles han comenzado la cuenta atrás para adaptarse al nuevo **Reglamento General de Protección de Datos** (RGPD) impuesto por la Unión Europea, que entró en vigor el 25 de mayo de 2016 y que **comenzará a aplicarse de forma obligatoria en la misma fecha de 2018.**

Su incumplimiento puede conllevar sanciones millonarias por lo que las pymes que no hayan tomado ya medidas para ajustar sus procedimientos a la norma europea deberán apurar este último año que resta de período de transición para ponerlas en marcha.

El Reglamento se aplicará a los responsables o encargados de tratamiento de datos, tanto si están establecidos en la Unión Europea como si no lo están, pero realizan tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos europeos, o como consecuencia de una monitorización y seguimiento de su comportamiento (apps, redes sociales, etc.). Así, el nuevo reglamento garantiza el mismo nivel de protección para todos los ciudadanos europeos, unificando las normativas de todos los países y regiones.

De forma general, las empresas tendrán ahora que interiorizar **los conceptos de privacidad por diseño y privacidad por defecto**, que las obliga a incorporar la privacidad en todo el ciclo productivo de un producto o servicio, desde su creación hasta su comercialización.

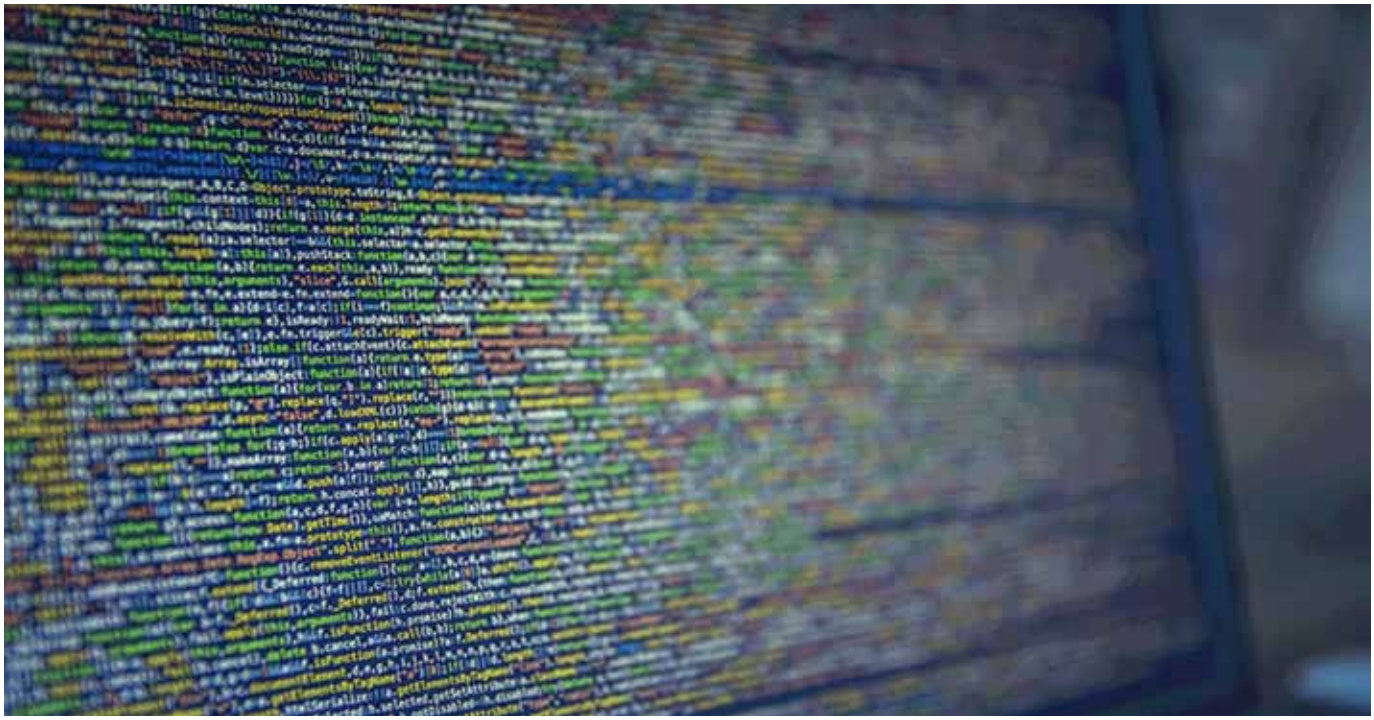
Cabe señalar que las organizaciones que están cumpliendo actualmente la Ley Orgánica de Protección de Datos (LOPD) parten, aún así, de una buena base para adaptarse al nuevo Reglamento, que modifica algunos aspectos e introduce nuevas obligaciones al respecto para adaptarse a las nuevas necesidades y exigencias derivadas de la transformación tecnológica.

Novedades:

1) El consentimiento: el Reglamento establece que el consentimiento sea **libre**, **informado**, **específico e inequívoco**, no pudiendo deducirse del silencio de la inacción de los ciudadanos. Así, prácticas aceptadas hasta ahora bajo el amparo de un consentimiento tácito, dejarán de serlo con la aplicación de la nueva norma.

En este sentido, las empresas deberán revisar los procedimientos y formularios de conformidad para adaptarlos a los nuevos requisitos del RGPD en cuanto al deber de informar. También tendrán que explicar la base legal para el tratamiento de datos, el plazo de retención de los mismos y especificar el lugar a donde se pueden dirigir las reclamaciones a las autoridades de protección de datos.

2) Información a los interesados: la información deberá proporcionarse por escrito con un **lenguaje claro y sencillo**, **de forma concisa**, transparente, inteligible y de fácil acceso, recomendando seguir **el modelo de información por capas o niveles**.



Se deberá suministrar la siguiente información:

- Base jurídica del tratamiento.
- Intención de realizar transferencias internacionales.
- Datos del delegado de protección de datos.
- Elaboración de perfiles.

La LOPD solo exige que se facilite de modo expreso, preciso e inequívoco.

3) Responsabilidad proactiva: las organizaciones deberán analizar qué datos trata, con qué finalidad y qué operaciones de tratamiento realizan para adoptar medidas preventivas que garanticen el cumplimiento del Reglamento (protección de datos por defecto, evaluaciones de impacto sobre protección de datos, notificación de violaciones de seguridad de datos…).

4) Nuevos derechos: el nuevo reglamento incorpora a los derechos Arco (acceso, rectificación, cancelación y oposición) el derecho al olvido, el derecho de limitación de tratamiento y el derecho a la portabilidad, mejorando el poder de las personas sobre sus datos personales establecido en la LOPD.

a) El derecho al olvido: posibilita que los ciudadanos europeos puedan solicitar a los responsables del tratamiento de datos que sus datos sean eliminados. No está considerado como un derecho autónomo sino como una consecuencia de los derechos de cancelación u oposición en el entorno online. Los usuarios podrán solicitar el bloqueo en buscadores de enlaces que dirijan a informaciones obsoletas, incompletas, falsas, irrelevantes o carentes de interés público.

b) Derecho de limitación de tratamiento: permite que el usuario pueda limitar el tratamiento de sus datos en el caso de que exista inexactitud o ilicitud en el tratamiento de los datos, para la defensa de reclamaciones o en caso de oposición del interesado -mientras se verifica si procede atender su solicitud-.

c) El derecho de portabilidad: permite que una persona que ha cedido sus datos a un responsable de tratamiento pueda recibir esos mismos datos en un formato de uso común, estructurado y de lectura rápida, que haga posible su transmisión al responsable de datos de otra empresa u organización. Este derecho facilita el flujo de datos personales, facilitando trámites como el cambio de proveedor.

5) Notificación de "violaciones de seguridad" de datos:
Establece que se debe notificar a las autoridades la fuga de datos en un plazo de 72 horas, desde que se origina. También deberán ser informados los ciudadanos, si supusiese un perjuicio significativo para ellos.

6) Ventanilla única:
Las empresas con sedes en varios países de la Unión Europea deberán responder ante la autoridad de protección de datos del país en el que tengan su sede principal. Esta autoridad de protección de datos nacional actuará como ventanilla única para todas las actividades que las empresas desarrollen, indistintamente del país en el que se lleven a cabo. De hecho, serán las agencias de protección de datos nacionales quienes continúen recibiendo las denuncias, realizando las investigaciones e imponiendo sanciones.

En caso de discrepancias de carácter transfronterizo, se podrá acudir al Comité Europeo de Protección de Datos, que integra a los directores de todas las autoridades de protección de datos de la Unión Europea.

7) Obligaciones del encargado de datos:
La responsabilidad sobre el tratamiento de datos sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad. Está obligado a:

- Mantener un registro de actividades de tratamiento.
- Tomar medidas de seguridad.
- Nombrar a un delegado de protección de datos en los casos previstos por el RGPD.

8) Elección del encargado de tratamiento:
Las empresas deberán seleccionar encargados que ofrezcan garantías a la hora de aplicar las medidas técnicas y organizativas exigidas por el RGPD. Este requisito se aplica también en caso de subcontratar el tratamiento. Además, las relaciones entre el responsable y el encargado deben formalizarse en un contrato o en un acto jurídico. Los contratos concluidos con anterioridad a la aplicación del RGPD deben modificarse y adaptarse a lo que marca el Reglamento.

9) Transferencias internacionales:

Los datos se podrán comunicar fuera de la Unión Europea si tienen como destino países, territorios o sectores que ofrecen un nivel de protección adecuado o si se trata de una excepción por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales, aún cuando no se cuenta con las garantías de protección exigidas.

10) Protección de los menores de edad:

Será necesario el consentimiento de los padres para recoger, procesar o almacenar datos de menores de 16 años. Esta edad podría ser modificada por la legislación interna de los países miembros de la UE, siempre que no sea menor de 13 años.

11) Datos de especial protección:

Se endurecen las medidas aplicadas a datos que requieren especial protección como datos sanitarios, biométricos, raciales o ideológicos.

12) Sanciones:

El RGPD introduce también cambios en el régimen sancionador, que se endurece en comparación con el de la LOPD e incrementa las cuantías de las infracciones.

Así, prevé la posibilidad de sancionar las infracciones con multas administrativas de 10 y 20 millones de euros como máximo, según el tipo en el que se encuadren de los apartados 4 o 5 del artículo 83 del Reglamento, o de una cuantía equivalente al 2% o el 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, si se trata de una empresa. Una medida que pretende disuadir a las organizaciones de cometer las llamadas "infracciones rentables".

En función del artículo del RGPD vulnerado, las sanciones pueden ser de:

- **Hasta 10 millones de euros o el 2% del volumen de negocio anual global del ejercicio financiero anterior:**

• No cumplir con las condiciones relativas al consentimiento de menores.
• No aplicar medidas técnicas y organizativas por defecto.
• No disponer de registro de actividades de tratamiento.
• No notificar brechas de seguridad.
• No realizar la evaluación de impacto.
• No designar DPO (Delegado de Protección de Datos).

- **Hasta 20 millones de euros o el 4% del volumen de negocio anual global del ejercicio financiero anterior:**

• No cumplir con los principios del RGPD.
• No cumplir con los derechos de los afectados.
• No cumplir con los requisitos para la transferencia internacional de datos.
• No cumplir con la resolución de la Autoridad de control.

Calixto Escariz, S.L.U.
despacho@calixtoescariz.com
www.calixtoescariz.com